Technical Cybersecurity

Binary Exploitation: The Stack

Binary Exploitation

We've discussed the stack

- We understand how it works and where things are placed

Time to use that info!

- We have some idea of how we can wrest program control from the running code
- Let's see how we do it

Approach

Our basic approach

- Create a flawed program
- This way you can see what NOT to do in your own code

Exploit the program

- We'll pass command line arguments into the program that will cause a failure

Moving to 32-bit

We'll be working in 32-bit for now

- Stack overflows are harder on 64-bit
- Most IoT code uses 32-bit or less today anyway

Binary debugging

- You'll learn to debug core files!
- Other debugger tricks
- Address Tracing
- Stack analysis

Let’s go!